Ministry of Higher Education
And Scientific Research
AL-Qadisiya University
College of Education
Department of Mathematics

The MATRU Cryptosystem

To the Council of the college of Education, AL-Qadisiya University, part of the requirements for obtaining a bachelor's degree in mathematics science

Submitted by

Furqan Farhan Jehad

1439A.H 2018A.D

بسم اللّه الرحمن الرحيم

﴿ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ ﴾

صدق اللّه العلي العظيم

سورة يوسف: اية 76

Acknowledgement

Firstly, thanks for Allah for everything.

I would like to express my sincere appreciation to my supervisor Assit. Prof. Dr. Hassan Rashed Yassein for giving me the major steps to go on exploring the subject, and sharing with me the ideas related to my work.

Also, I would like to express my deep thanks to all my teachers of the Department of Mathematics, College of Education, University of AL-Qadisiyah especially, Dr. Mazin Omran Kareem head of the Department.

My deepest thanks go to my family for their immeasurable encouragement and prayer, and I know all the thanks words will never be enough to my friends for their support.

Forqan

2018

Abstract

In this thesis, three mathematical structures are proposed to be used as an alternative to NTRU based ring. The first is based on a new proposed algebra called Hexadecnion algebra, which is a non-associative, non-commutative and alternative, we call it HXDTRU. The proposed system is implemented, and its security and efficiency are analyzed. The second is based on para quaternion algebra with dimension four, which is non-commutative and associative, we call it PQTRU. Its suitability is proved through two propositions, and its security is demonstrated to be eight times greater than NTRU security. The third is based on another new algebraic structure to be used as an alternative to NTRU-mathematical structure called binary algebra. It is non-commutative and non-associative, we call it BITRU. Its security is demonstrated in comparing to NTRU.

Contents

Chapter 1

General Introduction

1.1 Introduction

Cryptography is the that applies complex mathematical to design a strong encryption method used for protecting information during transmission and storage [1]. Many public key cryptosystems have been developed since the Diffie Hellman seminal paper [2] has been presented in
1976. Most of them are based on two hard mathematical hard problems: the factorization and discrete logarithm problems,(e.g, RSA [3], ElGamal cryptosystem [4], ECC [5].and many others).From the practical point of view ,Most of these systems are costly because of space complexity and high computation. This problem can be overcome by looking for new fast cryptosystems based on different hard problems.

The Number Theory Research Unit (NTRU) public Key cryptosystem is on of the cryptosystems founded in 1996 by three mathematicians, Jeffery Hoffstein, Joseph Silverman, and Jill Piper [6]. The basic collection of objects used by the NTRU public key cryptosystem happens in truncated polynomial ring of degree $N-1$ with integer coefficients belonging to z[x]/9x^N -1).

The NTRU is first public key cryptosystem that doesnot depend on the aforementioned mathematical problems. In comparison with RSA and ECC cryptosystems, the NTRU is faster and has significantly smaller keys

During the past twenty years, NTRU analyzed carefully by the researchers are still fundamental key is supposed to be safe. Most sophisticated attacks against NTRU are based on techniques for reducing the . Two famous lattice, the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), have shown to be
among the NP- hard problems [7, 8, 9, 10].

However, the problem of appear emerging NTRU classified as a Convolution Modular Lattice (CML) and it did not specify, so far, whether the structure of the League of CML will help to reduce the complexity of the CVP or SVP. The consideration of this issue in the new versions of NTRU [11, 12].

Computational efficiency along with low cost implementation have turned NTRU into a very suitable choice for a large number of applications such as resource constrained device, portable device, mobile phone and embedded system [13, 14].

1.2 Literature Review

Based on the same construction structure of NTRU, many good alternatives to it were introduced since that time. They were designed to improve its performance by replacing the original polynomial ring.

All of them aimed to design of NTRU like cryptosystem with short key size and secure against lattice attack. Some of these attempts are presented as follows:

- In 1997, Coppersmith and A Shamir [15] discuss some lattice attacks against NTRU cryptosystem and introduce these attacks, a non-commutative algebra can be considered for the underlying algebra.
- In 2002, Gaborit et al introduced CTRU based on the ring of the polynomials in one variable over a finite field[16]. For the same value of *N*, the speed of encryption and decryption of NTRU is the same as CTRU.
- In 2003, Proos [17] described an attack on NTRU. The attack uses decryption failures to reduce the size of the lattice problem that must be solved to recover the private key. In the same year, Graham et al. [18] presented a padding scheme suitable for cryptosystem with nonzero, but, trivial average–case chance of decryption failure.

- In 2005, Kouzmenko [19] showed that the CTRU is weak under a time attack and proposed the GNTRU cryptosystem based on Gaussian integers $Z[i]$ instead of Z or $F_2[x]$. In the same year, M. Coglianese and B.Goi [20]introduced an analog to the NTRU cryptosystem called the MaTRU. The MaTRU is based on a ring of all square matrices $K \times K$ with polynomial entries of order *n*. This improvement has a respectable speed by a factor of $O(n^2 k)$ over NTRU at the cost of a somewhat larger public key, another for MaTRU is that the new cryptosystem has the same bits number per message as instance of NTRU when $n^2 k = N$.
- In 2006, Slaibi [21] presented some improvements of the basic

1.3 Problem Statement

New terms such as closest vector problem (CVP) and the shortest vector problem (SVP), which have been illustrated as NP-hard problem, emerged, leading to a new hope for designing public key cryptosystem based on certain lattice hardness. A new cryptosystem called NTRU is proven computationally efficient and it can be implemented with low cost. With these characteristics, NTRU possesses advantage over others system that rely on number-theoretical problem in a finite field (e.g. integer factorization problem or discrete logarithm problem). These advantages make NTRU a good choice for many applications. Despite these advantages NTRU type cryptosystems have a decryption failure probability. It is a big challenge associated with such type of cryptosystem.

2.1 Introduction

This chapter briefly summarizes some of the basic concepts concerning algebra, polynomial ring, and truncated polynomial ring. It also presents some algorithms used for finding of the multiplication and multiplicative inverse of the polynomials in truncated polynomials ring, in the addition to the lattice based reduction and LLL reduced algorithm.

2.2. Algebra

Definition (2.2.1) [21]: A set V is said to be a vector space over a field F if V is an abelian group under addition (denoted by $+$) and, if for each $a \in F$ and $v \in V$, there is an element av in V such that the following conditions hold for all a, b in F and u, v in V:

1. $a(u+v) = au + av$
2. $(a+b)v = av + bv$
3. $(ab)v = a(bv)$
4. $1v = v$

The vector space members are called vectors and the field members are called scalar. The scalar multiplication is the operation that combines a vector v and a scalar a to produce the vector av .

Definition (2.2.2) [21]: A subset B of a vector space V over a field F is called a basis of V if:

1. B is linearly independent.
2. $B =$ span V.

Definition (2.2.3) [21]: let V be a vector space over a field F. If V has basis with n vectors then n is called the dimension of V, it is written as $\dim(V) = n$.

Definition (2.2.4) [21]: let A be a vector space over a field. A is said to be an algebra over F if there is a binary operation (multiplication)

$A \times A \rightarrow A$ denoted by $(a, b) \rightarrow a.b$ such that for all $a, b, c \in A$ and $\alpha \in F$, we have:

1. $a.(b + c) = a.b + a.c$
2. $(b + c).a = b.a + c.a$
3. $\alpha\,(a.b) = (\alpha a).b = a.(\alpha b)$.

The algebra A is commutative if $a.b = b.a$ for all $a, b \in A$, and it is associative if $a.(b.c) = (a.b).c$ for all $a, b, c \in A$.

Definition (2.2.5) [21]: The dimension of the algebra A is equal to the dimension of its vector space.

Example (2.2.6) [22]: Let $(Z_2, +_2, \cdot_2)$ be the field of integers modulo 2 then $A = \{\sum_{i=1}^{3} r_i e_i + \sum_{j=1}^{4} s_j n_j \,|\, r_i, s_j \in Z_2\}$ with multiplication Table (1) illustrates the algebra of dimension 7.

Table 1 (Multiplication operation)

	e_1	e_2	e_3	n_1	n_2	n_3	n_4
e_1	e_1	0	0	n_1	n_2	0	0
e_2	0	e_2	0	0	0	0	0
e_3	0	0	e_3	0	0	n_3	n_4
n_1	n_1	0	0	0	0	0	0
n_2	n_2	0	0	0	0	0	0
n_3	0	0	n_3	0	0	0	0
n_4	0	0	n_4	0	0	0	0

Definition (2.2.7) [23]: An algebra A over a field F is called division algebra if every non-zero element has a multiplication inverse.

Definition (2.2.8) [23]: An algebra A is alternative if it satisfies the right and left alternative identities $(y.x).x = y.(x.x)$ and $(x.x)y = x.(x.y)$ for all $x, y \in A$.

Lemma (2.2.9) [24]: (Moufang identities)

Every alternative algebra satisfies the following three identities:

1. $y((xz)x) = ((yx)z)y$
2. $(xy)(zx) = (x(yz))x$
3. $(x(yx))z = x(y(xz))$.

It is clear that every associative algebra is alternative.

2.3. Polynomial Ring

Definition (2.3.1) [24]: Let R be a ring, then a polynomial in the indeterminate x over the ring R is an expression of the form

$$f(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_2\, x^2 + a_1\, x^1 + a_0,$$

where $a_i \in R$, and $n \geq 0$. The element a_i is called the coefficient of x^i in $f(x)$. The degree of $f(x)$ is the largest integer n such that $a_n \neq 0$, it is denoted by deg $f(x)$, where a_n represents the leading coefficient of $f(x)$.

The set of all polynomials over a ring R may be regarded as the set R denoted by $R[x]$. Let $g(x) = b_n\, x^n + b_{n-1}\, x^{n-1} + \cdots + b_2\, x^2 + b_1\, x^1 + b_0$, the sum $f + g$ is defined by the rule:

$$f(x) + g(x = (a_n + b_n)\, x^n + \cdots + (a_1 + b_1)\, x^1 + (a_0 + b_0),$$

and the operation of multiplication in $R[x]$ takes the form

$$f(x) * g(x) = c_n\, x^n + \cdots + (a_1 + b_1)\, x^1 + (a_0 + b_0)$$

where

$$c_k = \sum_{i+j=k} a_i b_j = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0.$$

Theorem (2.3.2) [24]: The triple $(R[x], +, *)$ form a ring, known as the ring of polynomials over R. Furthermore, the ring $(R[x], +, *)$ is commutative with identity if and only if R is a commutative ring with identity.

Theorem (2.3.3) [24]: (Division Algorithm)

If $f(x), g(x) \in F[x]$, with $g(x) \neq 0$,then there exist unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

The polynomial $q(x)$ and $r(x)$ appearing in the representation

$f(x) = q(x)g(x) + r(x)$ given by the division algorithm are called, respectively, the quotient and the remainder of dividing $f(x)$ by $g(x)$.

Definition (2.3.5) [25]: If $g(x), h(x) \in F[x]$ then $g(x)$ is said to be congruent to $h(x)$ mod $f(x)$ if $f(x)$ divides $g(x) - h(x)$, it is denoted by

$g(x) \equiv h(x) \bmod f(x)$.

2.4. Truncated Polynomial Ring[i]s

The set of all polynomials of degree $N-1$ having integer coefficients is denoted by R_T, where

$$R_T = \{a_0 + a_1 x + \cdots + a_{N-2}x^{N-2} + a_{N-1}x^{N-1} \mid a_i \in Z\}.$$

The polynomials in R_T are added together in the usual way by simply adding their coefficient.

They are also multiplied in almost the usual manner, with one change after doing the multiplication, the power x^N should be replaced by 1 ($x^N \equiv 1$).

Let $g = b_0 + b_1 x + b_2 x^2 + \cdots + b_{N-2}x^{N-2} + b_{N-1}x^{N-1}$, the following is the general formula for polynomial multiplication in R_T

$$f * \mathrm{g} = c + c_1 x + c_2 x^2 + \cdots + c_{N-2}x^{N-2} + c_{N-1}x^{N-1}$$

where the k^{th} coefficient c_k is given by the formula

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k+1} b_{N-1} + a_{k+2} b_{N-2} + \cdots + a_{N-1} b_{k+1},$$

the k^{th}coefficient c_k is simply the product of the coefficients of f and the coefficients of g, except that first the coefficients of g are listed in reverse order and are rotated around k positions.

The above addition and multiplication rules make R_T as a ring, which is called the ring of truncated polynomial [26]. In terms of modern abstract algebra, the ring R is isomorphic to the quotient ring $Z[x]/(x^N - 1)$.

3.1. Introduction

Communications are the instrument of life in the present days. Therefore, it is necessary to find methods of sending information through a non-secure channel securely to preventing them from third party attacks. Cryptosystem based on the difficulty of integer factorization or the discrete logarithm problems are group-based cryptosystem, because the underlying hard problem involves only one operation.

In this chapter, we described NTRU public key cryptosystem which use polynomial algebra combined with the clustering principle based on elementary mathematical theory. NTRU naturally described using convolution polynomial rings, but the aforementioned hard mathematical problem can also be represented as closest vector problem or the shortest vector problem in lattice.

It also describes two NTRU like cryptosystems; which are the QTRU that is that constructed based on the quaternions algebra which is an alternative but non-associative, and OTRU, that is based on octonion algebra, which alternative but non-associative.

3.2. NTRU Cryptosystem

NTRU Cryptosystem is. It depends on the addition and multiplication in the ring of a truncated polynomial of degree N denoted by $[x]/(x^N - 1)$. This cryptosystem is described as follows:

Consider the truncated polynomial rings $K = Z[x]/(x^N - 1)$ where N is prime. Let $K_p = Z_p[x]/(x^N - 1)$ and $K_q = Z_q[x]/(x^N - 1)$ are denoted the rings of truncated polynomial modulo p, and q respectively, where p and q are integers number, such that p, q which are coprime, and p is much smaller than q.

An element in the rings $K, K_p, and\ K_q$ can be written either as $f = \sum_{i=0}^{N-1} f_i x^i$ or in the vector form $f = [f_0, \dots, f_{N-1}]$.

Let d_f, d_g, d_m and d_p be constant integers less than N, these are the public parameters of the cryptosystem and determine the distribution of the coefficient of the polynomial. According to these constants, we consider the subsets $L_f, L_g, L_m\ and\ L_\emptyset \subset K$ of small polynomial as defined in Table 3.1.

Table 3.1 (Subsets definitions of NTRU)

Notation	Definition
L_f	$\{f \in K \mid f$ has d_f coefficients equal to +1, $(d_f - 1)$ coefficients equal to -1, and the rest are 0$\}$
L_g	$\{g \in K \mid g$ has d_g coefficients equal to +1, d_g coefficients equal to -1, and the rest are 0$\}$
L_r	$\{r \in K \mid r$ has d_r coefficients equal to +1, d_r coefficients equal to -1, and the rest are 0$\}$
L_m	$\{m \in K \mid$ coefficients of m are chosen modulo p between $-p/2$ and $p/2\}$

In NTRU cryptosystem, the random polynomials are required to be generated with the condition that all of its coefficients are $\{-1, 0, 1\}$.

The NTRU Cryptosystem can be described through three phases.

1) Key Generation phase

The public key and the private key are generated such that; the sender first randomly choose two small polynomials f and g from L_f and L_g, respectively, such that f must be invertible modulo p and q their inverses are denoted by F_p and F_q, respectively, such that $f * F_p = 1$ and $f * F_q = 1$.

However, a new polynomial $f$should be chosen if probable f is not invertible.

The inverse of f over K_p and K_q are computed by the extended Euclidian algorithm. the public key h is computed in following manner

$h = F_q * g \ (mod \ q)$ …… (1)

while f, g, F_p andF_q are kept private.

2) Encryption phase

To convert an input message to aciphertext, we follow the following steps:

1. select randomly $r \in L_r$, called the biling polynomial or (ephemeral key)
2. The cipher text is computed as follows

$$e = ph * r + m(\text{ mod } q)\text{........ (2)}$$

The NTRU encryption process N addition and N^2 multiplication mod q.
Decryption phase

After receiving the ciphertext e, the original message is obtained through the following steps:

1. Multiplying the received polynomial e by the private key f mod q

$$f * e \text{ (mod q)} = f * (ph * r + m) \text{ (mod q)}$$
$$= pf * h * r + f * m \text{ (mod } q)$$
$$= pf * F_q * g * r + f * m \text{ (mod } q)$$
$$= pg * r + f * m \text{ (mod } q) \quad \ldots\ldots. \quad (3)$$

2. The coefficient of (3) should be adjusted to lie in the interval $(-q/2, q/2]$. Therefore, it does not changes if its coefficients are reduced mod q.
3. The receiver computes the polynomial as follows:

$$b = pg * r + f * m \text{ (mod } p)$$
$$= f * m \text{ (mod } p)$$

4. To get the message m, it is enough to multiply b in step 3 by F_q and the resulting coefficient are adjusted to lie in the interval $(-q/2, q/2]$.

In the NTRU decryption process two truncated polynomial multiplication are performed hence, the encryption speed is twice faster than the decryption

3.2.1. Successful Decryption

The successful decryption in NTRU cryptosystem depends on whether $|pg * r + f * m|_\infty < q$ or not.

By a few simple probabilistic calculations, such that, the coefficient of $f * m$ and $g * r$ have normal distribution around zero and the approximate bound for the successful decryption probability can be calculated as follows:

$$\text{Pr(successful decryption)} = (2\varphi\left(\frac{q-1}{2\sigma}\right) - 1)^N$$

here φ denotes the distribution of the standard normal variable and

$$\sigma = \sqrt{\frac{36dfdg}{N} + \frac{8df}{6}}.$$

4 The MaTRU cryptosytem

4.1 Notation

The MaTRU cryptosystem operates in the ring $\mathbf{M}$ of k by k matrices of elements in the ring $\mathbf{R} = \mathbb{Z}[X]/(X^n - 1)$. The ring $\mathbf{R}$ consists of polynomials with degree at most $(n-1)$ having integer coefficients. Multiplication and addition of polynomials in $\mathbf{R}$ is done in the usual manner, but exponents of X are reduced modulo n. Matrix multiplication in $\mathbf{M}$ is denoted using the $*$ symbol.[20]

Besides n and k, MaTRU also uses the parameters $p, q \in \mathbb{N}$. The numbers p and q may or may not be prime, but they must be relatively prime. In general, p is much smaller than q; in this paper, for ease of explanation, we stick to $p = 2$ or $p = 3$ and q in the range of 2 . When we say we perform a matrix multiplication modulo p (or q), we mean that we reduce the coefficients of the polynomials in the matrices modulo p (or q).We define the *width* of an element $M \in \mathbf{M}$ to be $|M| = (\max_{\text{polys. } m \text{ in } M} \text{coeff. in } m) - (\min_{\text{polys. } m \text{ in } M} \text{coeff. in } m)$. The width of M is the maximum coefficient in any of its k^2 polynomials minus the minimum coefficient in any of its polynomials. We say a matrix $M \in \mathbf{M}$ is *short* if $|M|_\infty \leq p$. When short matrices are multiplied together, we get a matrix which has a width which may be greater than p but is still almost certainly smaller than q; we call this matrix *pretty short*. The definitions for width and shortness apply similarly to polynomials in $\mathbf{R}$. For $r \in \mathbf{R}$, $|r|_\infty = (\max \text{ coeff. in r}) - (\min \text{ coeff. in r})$. The polynomial r is said to be short if $|r|_\infty \leq p$. We also define the *size* of an element $M \in \mathbf{M}$ to be $|M| = \sqrt{\sum_{\text{polys. } m \text{ in } M} \sum (\text{coeff. in } m)^2}$.

When defining some of the sets of short matrices below, we use the notation

$$\mathcal{L}(d) = \left\{ M \in \mathbf{M} \;\middle|\; \begin{array}{l} \text{for } i = \left\lceil -\frac{p-1}{2} \right\rceil \ldots \left\lceil \frac{p-1}{2} \right\rceil, i \neq 0, \text{ each polynomial} \\ \text{in } M \text{ has on average } d \text{ coefficients equal to } i, \\ \text{with the rest of the coefficients equal to } 0. \end{array} \right.$$

For example, if $p = 3$ and $n = 5$, then $\mathcal{L}(2)$ consists of all matrices of polynomials where on average each polynomial has 2 coefficients equal to 1, 2 coefficients equal to -1, and 1 coefficient equal to zero. Or, if we had $p = 2$ and $n = 5$, then $\mathcal{L}(2)$ consists of all matrices of polynomials where on average each polynomial has 2 coefficients equal to 1 and 3 coefficients equal to zero.

The parameters for MaTRU consist of the four integers (n, k, p, q) described above and the five sets of matrices $(\mathcal{L}_f, \mathcal{L}_\Phi, \mathcal{L}\quad) \subset \mathbf{M}$. These sets have the following meanings and compositions:

Set	Elements	Description	Composition
$\mathcal{L}_f$	f, g	Compose private key	Short; see (2) below
$\mathcal{L}_\Phi$	Φ, Ψ	Random matrices applied for each encryption	Short; see (2) below
$\mathcal{L}_A$	A, B	Used to construct f, g, Φ, Ψ	Short; see (1) below
$\mathcal{L}_w$	w	Used to construct public key	Short
$\mathcal{L}_m$	m	Messages	Short; see (3) below

1. $\mathcal{L}_A$ consists of all matrices $C \in \mathbf{M}$ such that C^0, C^1 are linearly independent modulo q; and for short $c_0, \ldots, c_{k-1}$ is short. Section 3.2 describes the exact nature of $\mathcal{L}$ that satisfies these conditions.
2. $\mathcal{L}_f$ and $\mathcal{L}_\Phi$ consist of all matrices $D \in \mathbf{M}$ constructed such that, for $C \in \mathcal{L}_A$ and short $c_0, \ldots, c_{k-1} \in \mathbf{R}$, $D = \sum_{i=0}^{k-1} c$. Additionally, matrices in $\mathcal{L}_f$ must satisfy the requirement that they have inverses modulo p and modulo q.

3. The set of messages $\mathcal{L}_m$ consists of all matrices of polynomials with coefficients modulo p. We therefore express

$$\mathcal{L}_m = \left\{ M \in \mathbf{M} \;\middle|\; \begin{array}{l} \text{polynomials in } M \text{ have coefficients} \\ \text{between } \left\lceil -\frac{p-1}{2} \right\rceil \text{ and } \left\lceil \frac{p-1}{2} \right\rceil \end{array} \right\} .$$

This means that each message contains $nk^2 \log_2 p$ bits of information.

4.2 Key Creation

To create a public/private key pair, Bob chooses two k by k matrices $A, B \in \mathcal{L}_A$. Next, Bob randomly selects short polynomials $\alpha_0, \alpha_1, \ldots \alpha_{k-1} \in \mathbf{R}$ and $\beta_0, \beta_1, \ldots \beta_{k-1} \in \mathbf{R}$. Bob then constructs the matrices $f, g \in \mathcal{L}_f$ by taking

$$f = \sum_{i=0}^{k-1} \alpha_i A^i \qquad \text{and} \qquad g = \sum_{i=0}^{k-1} \beta_i B^i \ .$$

As noted above in Section 2.1, the matrices f and g must have inverses modulo p and modulo q. This will generally be the case, given suitable parameter choices. We denote the inverses as F_p, F_q and G_p, G_q, where

$$\begin{array}{lcl} F_q * f \equiv I (\text{mod } q) & \text{and} & F_p * f \equiv I (\text{mod } p); \\ G_q * g \equiv I (\text{mod } q) & \text{and} & G_p * g \equiv I (\text{mod } p). \end{array}$$

Note that I is a k by k identity matrix. Bob now has his private key, (f, g), although in practice he will want to store the inverses F_p and G_p as well. Bob now selects a random matrix $w \in \mathcal{L}_w$, and constructs the matrix $h \in \mathbf{M}$ by taking

$$h \equiv F_q * w * G_q \qquad (\text{mod } q) \ .$$

Bob's public key consists of the three matrices, (h, A, B).

4.3 Encryption

To encrypt a message to send to Bob, Alice randomly generates the short polynomials $\phi_0, \phi_1, \ldots \phi_{k-1} \in \mathbf{R}$ and $\psi_0, \psi_1, \ldots \psi_{k-1} \in \mathbf{R}$. Alice then constructs the matrices $\Phi, \Psi \in \mathcal{L}_\Phi$ by taking

$$\Phi = \sum_{i=0}^{k-1} \phi_i A^i \qquad \text{and} \qquad \Psi = \sum_{i=0}^{k-1} \psi_i B^i \ .$$

Alice then takes her message $m \in \mathcal{L}_m$, and computes the encrypted message

$$e \equiv p(\Phi * h * \Psi) + m \qquad \pmod q \ .$$

Alice then sends e to Bob.

4.4 Decryption

To decrypt, Bob computes

$$a \equiv f * e * g \qquad \pmod q \ . \tag{1}$$

Bob translates the coefficients of the polynomials in the matrix a to the range $-q/2$ to $q/2$ using the centering techniques as in the original NTRU paper [8]. Then, treating these coefficients as integers, Bob recovers the message by computing

$$d \equiv F_p * a * G_p \qquad \pmod p \ .$$

4.5 Why Decryption Works

In decryption, from Eq. [1] Bob has

$$\begin{aligned} a &\equiv f * (p(\Phi * h * \Psi) + m) * g && \pmod q \\ &\equiv p(f * \Phi * F_q * w * G_q * \Psi * g) + f * m * g && \pmod q \end{aligned}$$

Although matrix multiplication is not generally commutative, f and Φ here do indeed commute:

$$\begin{aligned} f * \Phi &\equiv (\textstyle\sum_{i=0}^{k-1} \alpha_i A^i) * (\sum_{i=0}^{k-1} \phi_i A^i) && \pmod q \\ &\equiv \textstyle\sum_{i=0}^{k-1} \sum_{i \equiv j+\ell \pmod k} \alpha_j A^j \phi_\ell A^\ell && \pmod q \\ &\equiv \textstyle\sum_{i=0}^{k-1} \sum_{i \equiv j+\ell \pmod k} \phi_\ell A^{j+\ell} \alpha_j && \pmod q \\ &\equiv \textstyle\sum_{i=0}^{k-1} \sum_{i \equiv j+\ell \pmod k} \phi_\ell A^\ell \alpha_j A^j && \pmod q \\ &\equiv (\textstyle\sum_{i=0}^{k-1} \phi_i A^i) * (\sum_{i=0}^{k-1} \alpha_i A^i) \equiv \Phi * f && \pmod q \end{aligned}$$

Similarly, $g * \Psi \equiv \Psi * g \pmod q$. So, Bob now has that

$$a \equiv p(\Phi * w * \Psi) + f * m * g \qquad \pmod q$$

For appropriate parameter choices, $|a|_\infty \leq q$. Then, treating the polynomials in this matrix as having coefficients in $\mathbb{Z}$, Bob can take those coefficients modulo p, leaving $f * m * g \pmod p$. The original message is then recovered by left-multiplying by F_p and right-multiplying by G_p.

5 Parameter Selection

5.1 Selection of pairs (f, g) and (Φ, Ψ)

We define d_f and d_ϕ such that

$$\mathcal{L}_f = \mathcal{L}(d_f) \qquad \text{and} \qquad \mathcal{L}_\Phi = \mathcal{L}(d_\phi) \ .$$

Since the matrices A and B are public, the security of f, g, Φ, and Ψ necessarily depends on the difficulty of discovering the short polynomials α_i, β_i, ϕ_i, and ψ_i. For this reason, we want to maximize the number of possible choices for these polynomials. We therefore commonly select

$$d_f \approx \frac{n}{p} \qquad \text{and} \qquad d_\phi \approx \frac{n}{p} \ .$$

See section 4.1 for precise brute force security calculations.

Remark 1. A matrix f in the ring $\mathbf{M}$ will be invertible modulo p and q, only if the correspond matrix determinant det_f, which is in the ring $\mathbf{R}$, is also invertible modulo p and q. In practice, this is impossible if $det\ (1) = 0$ (the sum of the coefficient values of the determinant polynomial is equal to 0). So we must re-select one or more of the polynomial elements in f if this condition was not fulfilled.

5.2 Selection of A and B

A main concern in generating the matrices f and Φ (and likewise, g and Ψ) is that they must not only commute, but they should also be short. Shorter matrices ensure that $|p(\Phi * w * \Psi) + f * m * g|_\infty$ will be smaller, which will allow us to reduce q and valid ciphertexts will be decipherable.

To achieve this, we select A and B to be *permutation matrices.* A permutation matrix is a binary matrix (i.e. consisting of only the scalars 0 and 1) such that there is exactly one 1 in each row and column with all 0s elsewhere. Since A and B have the additional requirement that the sets $A^0, \ldots, A^{k-1}$ and $B^0, \ldots, B^{k-1}$ are both linearly independent, we have that

$$\sum_{i=0}^{k-1} A^i = \sum_{i=0}^{k-1} B^i = \begin{pmatrix} 1 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 1 \end{pmatrix} \ .$$

This implies that each row and column of f will contain some permutation of $\alpha_0, \ldots, \alpha_{k-1}$, meaning that each α_i will appear k times in f. An analogous situation exists for g, Φ, and Ψ.

Using the common choice of $d_f \approx d_\phi \approx \frac{n}{p}$, we have that

$$|f| \approx \sqrt{k^2|\alpha_i|^2} \approx \sqrt{\frac{(p-1)nk^2}{p}} \approx |g| \approx |\Phi| \approx |\Psi| \ .$$

5.3 Selection of w

Like f and g, w should also be chosen to be short in order to keep $|p(\Phi * w * \Psi) + f * m * g|_\infty$ small. For security reasons, it is important that w remain secret from an attacker. Therefore, in order to maximize the space of w we make

$$\mathcal{L}_w = \mathcal{L}\left(\left\lfloor \frac{n}{p} \right\rfloor\right) \ .$$

The size of w is then given by

$$|w| = \sqrt{\frac{(p-1)nk^2}{p}} \ .$$

Remark 2. Note that when w is chosen in this manner, on average $|w| \approx |m|$. This means that $|\Phi * w * \Psi| \approx |f * m * g|$.

6 Security Analysis

6.1 Brute Force Attacks

To find a private key by brute force, an attacker must try all possible short pairs of matrices (f, g) to find one such that $f * h * g$ is also short. Since the matrices A and B are public, f and g are determined by the $2k$ polynomials $\alpha_0, \ldots, \alpha_{k-1}, \beta_0, \ldots, \beta_{k-1}$. Each of these polynomials has degree $n-1$, so the number of possible (f, g) pairs is

$$\text{(key security)} \ = \left(\frac{n!}{(n-(p-1)d_f)!d_f!^{(p-1)}}\right)^{2k} . \tag{2}$$

Similarly, the encryption of a particular message is determined by the $2k$ polynomials $\phi_0, \ldots, \phi_{k-1}, \psi_0, \ldots, \psi_{k-1}$, so we have the same message security as Eq. [2] with replacing d_f by d_ϕ. Using a meet-in-the-middle attack, such as the method due to Odlyzko [18] used on the standard NTRU algorithm, assuming sufficient memory storage, the key and message security would be equal to the square root of the above values. Note that for the standard NTRU algorithm with the suggested parameters, the meet-in-the-middle attack is the most effective known attack.

References

[1] D. Denning. “Cryptography and data security”, Addison – Wisely Publishing Company, 1982.

[2] W. Diffie, M. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, vol.22, no.6, p.p.644-654, 1976.

[3] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signature and public key cryptosystems”, Communications of the ACM, vol. 21, no.2, p.p.120-126, 1978.

[4] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithm”, IEEE Transactions on Information Theory, vol. 31, no. 4, p.p. 469-472, 1985.

[5] R. Schoof “Elliptic curve over finite fields and the computation of square roots mod p”, Mathematics of computation, vol.44, no.170, p.p. 483-494, 1985.

[6] J. Hoffstein, J. Pipher, and J. Silverman, “NTRU: A ring based public key cryptosystem”, Proceeding of ANTS III, LNCS, Springer Verlag, vol.1423, p.p. 267-288, 1998.

[7] M. Ataji, “The shortest vector problem in 12 is NP-hard for randomized reduction”, Proceedings of the thirtieth annual ACM symposium on theory of computing, p.p. 10-19, New York, NY, USA, 1998.

[8] D. Micciancio, “The hardness of the closest vector problem with preprocessing”, IEEE Transactions on information theory, vol.47, no.3, p.p. 1212-1215, 2001.

[9] D. Micciancio, “The shortest vector problem is NP-hard to approximate to within some constant”, SIAM journal on computing, vol.30, no.6, p.p. 2008-2035, 2001.

[10] D. Micciancio and S. Goldwasser, “Complexity of Lattice Problems a cryptographic perspective ”, The Kluwer International series in Engineering and computer science, Kluwer Academic Publisher, Boston vol.671, no.6, p.p. 2008-2035, 2001.

[11] A. Mary and J. Silverman, “Dimension reduction methods for convolution modular lattice”, International Conferences on cryptography and lattice, London, UK, Springer-Verlag, p.p. 110-125, 2001.

[12] N. Howgrave, J. Hoffstion, J. Pipher and W. Whyte, “NTRU cryptosystems”, on estimating the lattice security of NTRU, 2005.

[13] D. V. Bailey, D. Coffin, A. Elbirt, J. H. Silverman, and A. D. Woodbury, “NTRU in constrained devices”, Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems. London, UK, Springer-Verlag, p.p. 262–272, 2001.

[14] T. Sobh, K. Elleithy, A. Mahmood and M. Karim, “Innovative Algorithms and Techniques in Automation Industrial Electronics and Telecommunications”, Springer Netherlands, 2007.

[15] D. Coppersmith and A. Shamir, “Lattice attacks on NTRU”, EUROCRYPT, p.p. 52-61, 1997.

[16] P. Gaborit J. Ohler, P. Soli, “CTRU, a polynomial Analogue of NTRU”, INRIA. Rapport de recherche, no. 4621, 2002.

[17] J. Proos, "Imperfect Decryption and an Attack on the NTRU Encryption Scheme", International Association for Cryptologic Research, vol. 2, p.p. 1-28, 2003.

[18] N. Graham, P. Nguyen, D. Pointcheval, J. Proos, J. Silverman, A. Singer and W. Whyte, "The Impact of Decryption Failures on the Security of NTRU Encryption", Advances in Cryptology - CRYPTO 2003, vol. 2729, p.p. 226-246, 2003.

[19] M. Coglianese, and B. Goi, “MaTRU: A new NTRU based cryptosystem”, Springer Verlag Berlin Heidelberg, p.p. 232-243, 2005.

[20] R. Kouzmenko, “Generalizations of the NTRU cryptosystem”, MS.C. Thesis, Polytechnique, Montreal, Canada, 2006.

[21] T.S. Slaibi, “Improved NTRU Cryptosystem”, Ph.D. thesis, University of Technology, 2006.

[22] P.R. Suri and P. Puri, “Application of LFSR with NTRU Algorithm”, Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, Springer, p.p. 369–373, 2007.

[23] A. Mersin, “The Comparative Performance Analysis of Lattice Based NTRU Cryptosystem with other Asymmetrical Cryptosystems”, M.Sc. Thesis, Graduate School of Engineering and Science of Izmir Institute of Technology, 2007.

[24] A. C. Atici, L. Batina, J. Fan, I. Verbauwhede and S. B. Yalcin, “Low-cost Implementations of NTRU for pervasive security”, IEEE Computer Society, Washington, 2008.

[25] E. Malekian, A. Zakerolhosseini and A. Mashatan, “QTRU: A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra ”, The ISC Int'l Journal of Information Security, vol. 3, no. 1 , p.p. 29–42, 2011.